17th February 2016 Moving onto Eaglesoft aka Patterson Dental

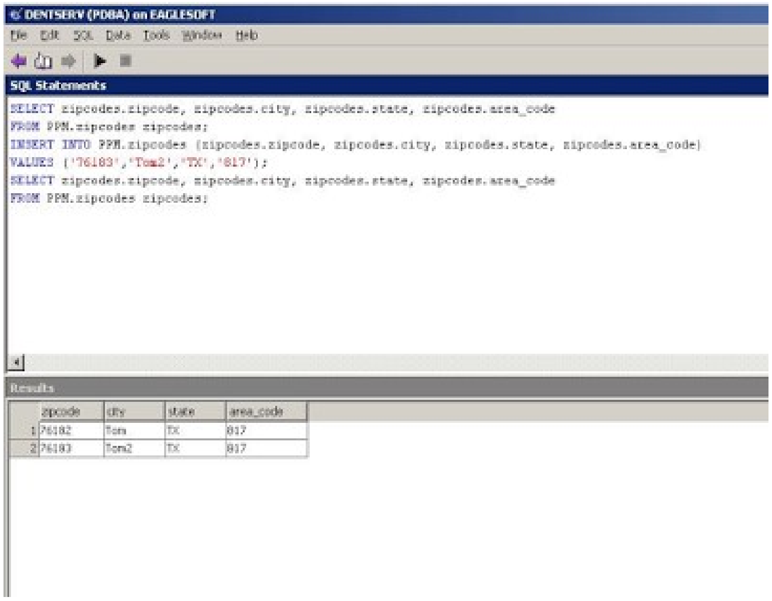
Moving onto Eaglesoft aka Patterson Dental

http://www.databreaches.net/22000-dental-patients-info-exposed-on-unsecured-eaglesoft-ftp-server/ [http://www.databreaches.net/22000-dental-patients-info-exposed-on-unsecured-eaglesoft-ftp-server/]
(Thanks Dissent!)
So I have been asking Eaglesoft since 2014 if they would improve the authentication of Eaglesoft. Eaglesoft uses Sybase iSQL Anywhere for its database.

How do they currently authenticate?
Currently for read access they use the default username and password dba and sql.

Do they support changing the backend database for reading AND writing?
I do not know but I plan on finding this out, I have asked US-CERT.

I have heard that if you want to write to their database, they do charge money, which I find odd because they don't seem to take great efforts into protecting write access, which is exactly what I heard is supposed to cost money.


DENTSERV (PDBA) on EAGLESOFT
File Edit SQL Data Tools Window Help
SQL Statements
Results

```
SELECT zipcodes.zipcode, zipcodes.city, zipcodes.state, zipcodes.area_code
FROM PPM.zipcodes zipcodes;
INSERT INTO PPM.zipcodes (zipcodes.zipcode, zipcodes.city, zipcodes.state, zipcodes.area_code)
VALUES ('76183','Tom2','TX','817');
SELECT zipcodes.zipcode, zipcodes.city, zipcodes.state, zipcodes.area_code
FROM PPM.zipcodes zipcodes;
```

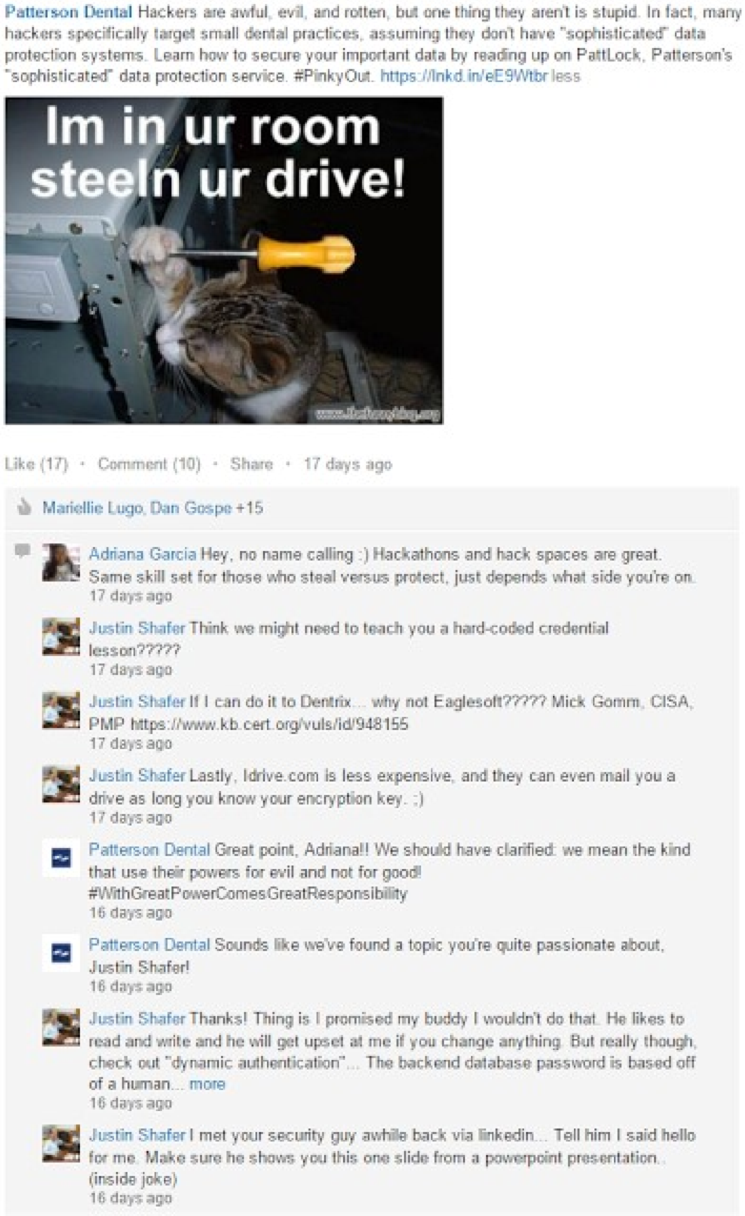
	zipcode	city	state	area_code
1	76182	Tom	TX	817
2	76183	Tom2	TX	817

[https://1.bp.blogspot.com/-gBAq2KYNZbk/Vrg8KVpFf3I/AAAAAAAABAs0/zMmTSpw0EdE/s1600/1.png]

I met their security guru Mike Snead via LinkedIn. He wanted to connecte with me and told me he liked my work regarding Dentrix. I thanked him and then said something he probably didn't like. I told him he had until Eaglesoft 18 to fix the authentication. He disconnected from me and I guess people in Dentistry are indignant so I am not that surprised.

I noticed this great post by Patterson (whom I like, don't get me wrong) on LinkedIn.

"Hackers are awful, evil, and rotten, but one thing they aren't is stupid. In fact, many hackers specifically target small dental practices, assuming they don't have "sophisticated" data protection systems. Learn how to secure your important data by reading up on PattLock, Patterson's "sophisticated" data protection service. #PinkyOut"



Patterson Dental Hackers are awful, evil, and rotten, but one thing they aren't is stupid. In fact, many hackers specifically target small dental practices, assuming they don't have "sophisticated" data protection systems. Learn how to secure your important data by reading up on PattLock, Patterson's "sophisticated" data protection service. #PinkyOut. https://lnkd.in/eE9Wtbr less

Like (17) · Comment (10) · Share · 17 days ago

Mariellie Lugo, Dan Gospe +15

Adriana Garcia Hey, no name calling :) Hackathons and hack spaces are great. Same skill set for those who steal versus protect, just depends what side you're on.
17 days ago

Justin Shafer Think we might need to teach you a hard-coded credential lesson?????
17 days ago

Justin Shafer If I can do it to Dentrix... why not Eaglesoft????? Mick Gomm, CISA, PMP https://www.kb.cert.org/vuls/id/948155
17 days ago

Justin Shafer Lastly, Idrive.com is less expensive, and they can even mail you a drive as long you know your encryption key. ;)
17 days ago

Patterson Dental Great point, Adriana!! We should have clarified: we mean the kind that use their powers for evil and not for good! #WithGreatPowerComesGreatResponsibility
16 days ago

Patterson Dental Sounds like we've found a topic you're quite passionate about, Justin Shafer!
16 days ago

Justin Shafer Thanks! Thing is I promised my buddy I wouldn't do that. He likes to read and write and he will get upset at me if you change anything. But really though, check out "dynamic authentication"... The backend database password is based off of a human... more
16 days ago

Justin Shafer I met your security guy awhile back via linkedin... Tell him I said hello for me. Make sure he shows you this one slide from a powerpoint presentation.. (inside joke)
16 days ago

[https://1.bp.blogspot.com/-obsimCdpYOs/Vrg-IzhxLNI/AAAAAAAABAtI/co1ze9ctMm0/s1600/3.png]

I thought about this and realized I most likely wasn't being taken seriously. Last week I went to an office that was giving out the 2Wire WPA2 key to PATIENTS (key=office phone number?). This offices has Eaglesoft. Somehow FEAR is the only thing that seems to work in Dentistry so.....

Other then spending time on how Eaglesoft authenticates, I noticed a free Eaglesoft 16 Developer License was on the Eaglesoft FTP site. This led to me wondering: What other careless mistakes have they put on their FTP Server?

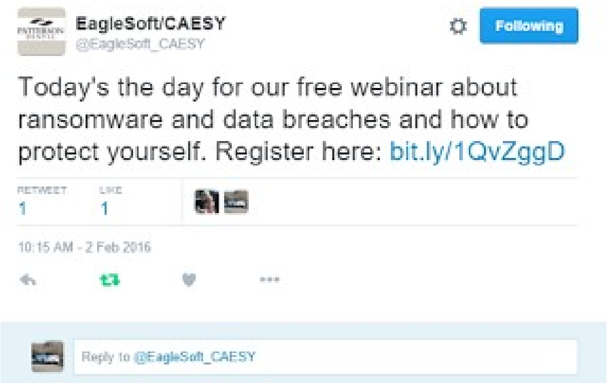
OH... Let me tell you.

1. A file called Dental.Log which is a transactional log file without the actual Dental.DB file to go along with it. I converted the dental.log file to dental.sql and discovered patient data with over 5000 patients. The patients belong to Massachusetts General Hospital.
http://www.massgeneral.org/dental/doctors/ [http://www.massgeneral.org/dental/doctors/]

2. A Recall Report from ES that was converted to PDF. This file belonged to a Dental office in Canada. There are over 2300 patients in this file. The SSN is not present, but insurance info, balances, and patient alerts are present.

3. An entire Eaglesoft Database was also present. This database was to an office in Canada and has a little over 15 thousand patients in the database.

This is all pretty sad, in a way. Apparently they just finished having a seminar February 2nd over "how to protect yourself from a data breach"



EagleSoft/CAESY
@EagleSoft_CAESY

Following

Today's the day for our free webinar about ransomware and data breaches and how to protect yourself. Register here: bit.ly/1QvZggD

RETWEET 1 LIKE 1

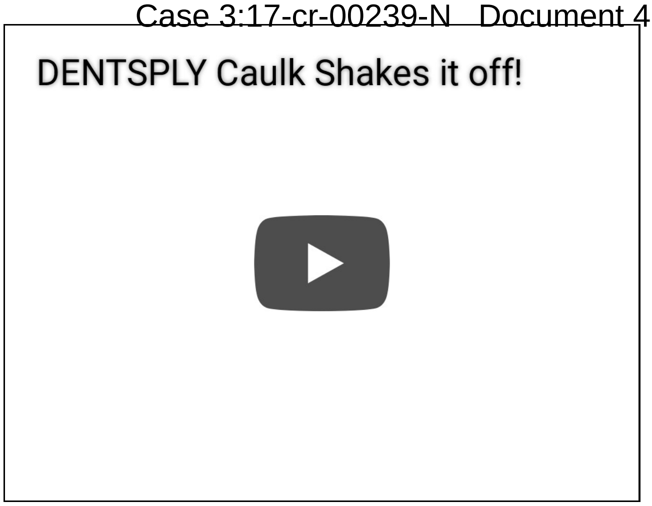
10:15 AM - 2 Feb 2016

Reply to @EagleSoft_CAESY

[https://2.bp.blogspot.com/-TVAvaqwkJMs/VrhAN2lFfXI/AAAAAAAABAtY/LFsSLP61C_8/s1600/4.png]

I hope SOMEONE at Patterson Dental or Eaglesoft knows I mean business, and the only HARM that can happen in not fulfilling our wishes, is what can happen to the generation that follows after us. It should be VERY CLEAR now.

#PinkyOut



Hints!

http://www.opendental.com/OpenDentalDocumentation15-4.xml#userod [http://www.opendental.com/OpenDentalDocumentation15-4.xml#userod]

http://www.opendental.com/manual/securitymysql.html [http://www.opendental.com/manual/securitymysql.html]

http://opendentalsoft.com/forum/viewtopic.php?f=2&t=4700 [http://opendentalsoft.com/forum/viewtopic.php?f=2&t=4700]

Posted 17th February 2016 by Justin Shafer

2 View comments

agamoto February 22, 2016 at 10:14 AM

Yeah, this is pretty wide open and ridiculous. I'm sure they'll say it's up to the client to protect their own network, but they really could make things a hell of a lot easier by tweaking a few things here. While they're at it, they may want to use a version of SQL Anywhere that supports VSS db quiescing so the db doesn't have to be stopped to get a clean backup. Not requiring local administrators/"power users" on the workstations would be a nice touch too.

Reply

Replies

Justin Shafer February 23, 2016 at 2:58 AM

VSS would be cool. The do have a dbbackup.exe that can be used, but that tool is just for SQLAnywhere. I remember because the credentials were dba and sql. =)

Reply

Enter your comment...

Comment as: J (Google)

Sign out

Publish **Preview**

□ Notify me